

IT Handbook Presentation Business Continuity Planning Booklet

Visual

Narrative

1.

IT Handbook Presentations

Business Continuity Planning Booklet 2008



The Information Technology Subcommittee of the FFIEC's Task Force on Supervision has released a revised version of the *Business Continuity Planning Booklet* of the Information Technology Examination Handbook.

2.

Business Continuity Planning



The Booklet has been updated to reflect technological and regulatory changes that have occurred since its first release in 2003.

This presentation highlights the general reorganization of, and material changes to, the Booklet.

3.

Management Issues

- **Enterprise-wide involvement**
- **Importance for all in-house and serviced activities**
- **Lessons learned from Hurricanes Katrina and Rita**
- **Pandemic planning**

The majority of these changes focus on management issues, such as:

- The need for enterprise-wide involvement in the business continuity planning process
- The importance of business continuity planning for all in-house and serviced activities of financial institutions
- Lessons learned from financial institutions that suffered damage from Hurricanes Katrina and Rita, and
- Pandemic planning

Visual

Narrative

4. **2003/2008 Differences**



Same overall goals!

Although the emphasis of this presentation is on highlighting differences between the 2003 and 2008 versions of the Booklet, the overall goal of the new version does not differ from that of the original.

5. **BCP Guidance**



Its purpose is to provide guidance to the financial services industry—guidance on the importance of BCP in establishing the basis for a financial institution’s ability to resume operations when the business has been disrupted unexpectedly.

6. **Crucial To National Economy**



Financial institutions play a crucial role in the national economy, and disruptions of services should be minimized in order to maintain public trust and confidence in the financial system.

7. **Continuing Focus**

- Enterprise-wide
- Process-oriented

Critical functions...

- Technology
- Business operations
- Testing
- Communication

While significant revisions have been made to the 2003 version, the focus of the Booklet continues to be an enterprise-wide, process-oriented approach that considers technology, business operations, testing, and communication BCP strategies to be as critical to the entire business as they are to the information technology department.

Visual

Narrative

8.

Booklet Content

- Introduction
- Board and Senior Management Responsibilities
- Business Continuity Planning Process
- Business Impact Analysis
- Risk Assessment
- Risk Management
- Risk Monitoring and Testing
- **Other Policies, Standards, and Processes**

Let's start our comparison by taking a look at the organization of the new Booklet. The narrative section of the new Booklet is divided into eight subsections:

- Introduction
- Board and Senior Management Responsibilities
- Business Continuity Planning Process
- Business Impact Analysis
- Risk Assessment
- Risk Management
- Risk Monitoring and Testing, and
- Other Policies, Standards, and Processes

9.

Other Policies, Standards and Processes

- Security standards
- Project management
- Change Control Policies
- Data Synchronization Procedures
- Crisis management
- Incident response
- Remote access
- Employee Training
- Notification standards
- Insurance
- Government- and Community-related issues

Those familiar with the earlier version of the Business Continuity Planning Booklet will notice an entirely new topic in this release—Other Policies, Standards, and Processes.

This new section provides information on:

- Security standards
- Project management
- Change Control Policies
- Data Synchronization Procedures
- Crisis management
- Incident response
- Remote access
- Employee Training
- Notification standards
- Insurance, and
- Government- and Community-related issues

10.

Hurricanes Katrina and Rita



The section also looks at some specific problems encountered by financial institutions affected by Hurricanes Katrina and Rita.

Where mitigating controls worked well for these institutions, the Booklet discusses the controls that were in place when these events occurred.

	<u>Visual</u>	<u>Narrative</u>
11.	<div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #000; margin-bottom: 5px;"> <p style="text-align: center; margin: 0;"><i>Mitigating Controls</i></p> <hr style="border: 1px solid #000; margin: 0;"/> <ul style="list-style-type: none"> – Change control policies – Data synchronization procedures – Employee training programs – Notification standards – Insurance – Government and community relationships </div>	<p>These include discussions of:</p> <ul style="list-style-type: none"> ▪ Change control policies ▪ Data synchronization procedures ▪ Employee training programs ▪ Notification standards ▪ Insurance, and ▪ Government and community relationships as they relate to BCP
12.	<div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #000; margin-bottom: 5px;"> <p style="text-align: center; margin: 0;"><i>Booklet Content</i></p> <hr style="border: 1px solid #000; margin: 0;"/> <ul style="list-style-type: none"> – Introduction – Board and Senior Management Responsibilities – Business Continuity Planning Process – Business Impact Analysis – Risk Assessment – Risk Management – Risk Monitoring and Testing – Other Policies, Standards, and Processes </div>	<p>You will also find significant changes in the Risk Monitoring and Testing section, which now incorporates the <i>Federal Reserve Testing Guidance</i>.</p>
13.	<div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #000; margin-bottom: 5px;"> <p style="text-align: center; margin: 0;"><i>Risk Monitoring and Testing</i></p> <hr style="border: 1px solid #000; margin: 0;"/> <ul style="list-style-type: none"> – Requirements for internal versus third-party processing – Clarification of various testing methods </div>	<p>This revised section includes:</p> <ul style="list-style-type: none"> ▪ Additional guidance on testing requirements for applications and systems that are processed internally versus those that are processed by third party service providers, and ▪ Additional clarification of various testing methods

Visual

Narrative

14.

Appendices

- Appendix A: Examination Procedures
- Appendix B: Glossary
- Appendix C: Internal and External Threats
- Appendix D: Pandemic Planning
- Appendix E: Interdependencies
- Appendix F: Business Impact Analysis Process
- Appendix G: Business Continuity Plan Components
- Appendix H: Testing Program - Governance and Attributes
- Appendix I: Laws, Regulations, and Guidance

The BCP Booklet also provides some new and revised resources in the appendices.

The appendices now include a total of nine resources:

- Appendix A: Examination Procedures
- Appendix B: Glossary
- Appendix C: Internal and External Threats
- Appendix D: Pandemic Planning
- Appendix E: Interdependencies
- Appendix F: Business Impact Analysis Process
- Appendix G: Business Continuity Plan Components
- Appendix H: Testing Program - Governance and Attributes, and
- Appendix I: Laws, Regulations, and Guidance

Let's take a brief look at how the appendices have changed.

15.

Appendix A

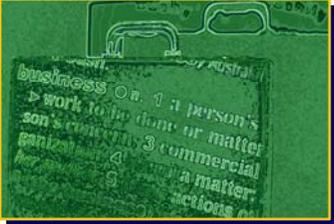


Examination Procedures

In the Examination Procedures, various changes reflect the Federal Reserve Testing Guidance and the FFIEC Guidance on Pandemic Planning and eliminate redundant work steps within the work programs. In addition, subheadings now enhance readability and ease of use.

16.

Appendix B



Glossary

The Glossary includes new terminology from the revised sections of the Booklet.

Visual

Narrative

17.

Appendix C



Internal and External Threats

Information was added to Appendix C- Internal and External Threats, to address problems experienced in Hurricanes Katrina and Rita.

18.

Internal and External Threats

- **Technical disasters**
- **Customer-related challenges**
- **Employee-related issues**
- **Electronic payment system providers**
- **Third-party providers**

This information relates to issues in such areas as:

- Technical disasters (e.g., communications failures)
- Customer-related challenges
- Employee-related issues
- Electronic payment system providers, and
- Third-party providers

19.

Appendix D



Pandemic Planning

A new section, based on interagency pandemic planning guidelines, was added to address the unique challenges posed by a pandemic, and content of an institution's pandemic plan, including:

Visual

Narrative

20.

Pandemic Planning

- A preventive program
- A documented strategy
- A comprehensive framework
- A testing program
- An oversight program

- A preventive program to reduce the likelihood that an institution's operations will be significantly affected by a pandemic event;
- A documented strategy that provides for scaling the institution's pandemic efforts so they are consistent with the effects of a particular stage of a pandemic outbreak;
- A comprehensive framework of facilities, systems, or procedures that provide the organization the capability to continue its critical operations in the event large numbers of the institution's staff are unavailable for prolonged periods;
- A testing program to better ensure the institution's pandemic planning practices and capabilities are effective and will allow critical operations to continue; and
- An oversight program to ensure ongoing review and updates to the pandemic plan.

21.

Appendix E



Interdependencies

Appendix E includes new information addressing interdependencies associated with telecommunications infrastructure issues such as single points of failure and related diversity guidelines.

22.

Interdependencies

- Telecommunications issues
- Liquidity concerns
- Transaction processing report distribution
- Due diligence requirements
- Guidelines on internal systems and business processes

Other expansion relates to interdependencies associated with:

- Telecommunications issues
- Liquidity concerns
- Transaction processing and report distribution, and
- Due diligence requirements

Based on recommendations from financial institutions' experiences during Hurricanes Katrina and Rita, guidelines were also added to address related internal systems and business process interdependencies.

Visual

Narrative

23.

Appendix F



Business Impact Analysis Process

The new Appendix F is based on recommendations from small- to medium-sized financial institutions. This appendix provides these institutions with steps they can follow to complete the Business Impact Analysis process.

24.

Appendix G



Business Continuity Plan Components

Also new to the appendix section of the revised BCP Booklet is Appendix G, Business Continuity Plan Components. This information is based on interviews with financial institutions that suffered devastation from Hurricanes Katrina and Rita.

25.

Business Continuity Plan Components

- Availability of personnel
- Communications breakdowns
- Availability of systems
- Cash shortages
- Unfamiliarity with manual operations

The most significant problems cited by this group related to the:

- Availability of personnel
- Communications breakdowns between financial institution employees, regulators, and service providers
- Availability of telecommunications systems
- Shortages of cash, and
- Employee unfamiliarity with manual operations

Thus, Appendix G outlines strategies to mitigate these types of potential problems, should a financial institution experience a disaster.

Visual

Narrative

26.

Appendix H



Testing Program—Governance and Attributes

The new material in Appendix H was added to incorporate the Federal Reserve Testing Guidance, which includes testing expectations based on the *Interagency Paper on Sound Practices to Strengthen the Resilience of the US Financial System*.

27.

Appendix I



Laws, Regulations, and Guidance

The list of laws, regulations, and guidance related to BCP has also been updated to provide internal and external resources to examiners in each of the five FFIEC agencies.

28.

Business Continuity Planning Booklet 2008



- Feedback from examiners and financial institutions
- New technology
- New regulations and guidance
- Lessons learned from catastrophic events

As you work with the 2008 version of the *Business Continuity Planning Booklet*, you will find that the comprehensive information on business maintenance, resumption, and recovery that was available in the 2003 version has been enhanced. These enhancements are based on feedback from examiners and financial institutions, on new technology, regulations and guidance, and on lessons learned from the catastrophic events that occurred since the issuance of the 2003 version of the Booklet.